Managing & Assessing
Reliability, Availability, and Maintainability of Systems: A Guide to Action

D. P. Gaver

P. A. Jacobs

E. A. Seglie

1. Reliability

Reliability generally refers to how, why, and when system hardware and software failures occur. A system is reliable if malfunctions or failures occur infrequently, and have small impact on mission success. Otherwise it is unreliable. The degree of reliability and types of failure are important and should be quantified. This is done using the ideas of *probability*. Reliability is the probability of failure free performance under stated conditions. Thus reliability cannot be *measured* independent of performance. (However, during development improvements in reliability can be facilitated with much less than a fully realistic operational environment.)

The first objective of testing is to discover and help remove failure modes of operational importance. Reliability can thus improve but can also decline if the "removed" is…

Failure is best looked at as any failure to achieve mission success.

A failure mode is an identifiable weakness in system design, manufacture, and typical field usage reduces the chance of mission success. A failure mode is a failure whose specific corrective action is different from other identified corrective actions. This definition avoids lumping failures with different causes or solutions together merely because they affect the same component or part. There may be many failure modes in a subsystem, each with a different solution, and each of which should be tracked separately.

There are many types of failure modes…

To some extent, reliability can be managed by controlling the usage space, preventative maintenance, and inspection, self-monitoring.

Functional Failures –Failure Causes and Definitions - Relevant Metrics

Every mission failure should be examined to determine which equipments or interfaces contribute to that failure. *Some* of these may be reliability failures, and some may be failures of performance.

Introduction

Conditions that influence failures

Environment

Stress

System Reliability Design Objectives

Mission Reliability

Logistics Related Reliability

Mission Failures

System Failures

Its better to have a continuous measure then a categorical success/failure measure. The former will contain more information.

For one-shot systems

On demand reliability

For repairable systems

Reliability

- Miles
- Hours
- Usage
- On demand

- Frequency and Amount of scheduled maintenance time
- Frequency of Unscheduled maintenance actions

Unscheduled maintenance actions

Logistic Burden

- Spares/Materiel
- Manpower
- Time to Repair
- Downtime (logistic support)

Design Metrics

- New Components
- Federal Stock Number

The link to Availability

The link to Maintainability

Hardware Software and System Reliability

There is often a discussion of the cause of the failure as a hardware failure or a software failure. Often the failure is identified as a software failure and the claim for example is made that "It is only software, so there is no hardware risk exposed in the failure." This is, in general, an erroneous claim. The failure is a system failure; the solution may be a software fix or a hardware fix. When it is claimed that it is a software failure the implication is that the fix can be in software. This is a claim not a fact. Often the solution to "software failures" is a change in hardware. For example, personal computers running a particular software program crash the system over and over. This could easily be identified as a problem with the software. The fit is often to either assign more memory to the program or to increase the memory of the computer.

2. Availability

3. Maintainability

Maintenance Equipment

- Uniqueness of Equipment
- Contractor maintenance/Warranty

4. A Good RAM Program

This guide is designed to help testers to contribute to improving, as well as assessing quantitatively, the reliability of a system. The goal in programs is constant improvement.

The contribution should begin at program inception and pave the way for a continued contribution throughout the life cycle of the system.

A good reliability program finds failure modes, analyzes the causes, evaluates possible corrective actions, and confirms the chosen corrective action or possible actions.

It is pro-active and helps anticipate problems. An early test is a success only if it finds something that leads to an improvement.

Every test should have a reliability aspect. Results should trigger inquiry as to causes of deficiencies.

Test and evaluation can start contributing even before there is hardware or software to test. It can test operational concepts, characterize the environment that the system will be in, the stresses on the system, utilizes known failure modes of similar systems, profit from understanding development problems of similar systems.

A primary function of T&E is to discover and help manage or control failure modes. Managing reliability can involve specification of usage, changing the inspections schedule, or preventive maintenance. These may have performance, availability, as well as maintainability implications. A further T&E task is to quantify maintenance, repair, and logistics needs to achieve the specified reliability.

The Reliability Program Inside Overall Program management

Reliability improvement requires top-level informed management attention.

A formal process is usually necessary. A proven process is Failure Reporting, Analysis, and Corrective Action System (FRACAS) and is controlled by a Failure Review Board (FRB) (See L.Crow—1998)

This includes Record keeping and Documentation in a form useful to program evolution and to other programs.

Reliability requirements definition and program definition

Reliability affects Mission Success (unreliability can degrade improved performance.) It affects the logistical burden the system imposes. It affects performance on the battlefield and the change that the system will get to the battlefield, and life cycle cost to the nation. The sophistication of the maintenance and the number of personnel needed to maintain the fleet. The spare parts that need to be carried, and the downtime when the system fails.

A useful evaluation tool to use at the earliest possible time is modeling the way in which the new system will work operationally, in a mission context (performance, reliability, and logistic support). This is useful even if the operational concepts are not set- in fact it is most useful before the concepts are set, and will contribute to getting good concepts.

Reliability in system design and source selection

There should be a reliability budget in the system design. This will add in component testing. In combination with the model of the system the reliability budget can help evaluate the need for redundancy, or special reliability requirements.

Different type so f systems

Repairable Systems / Continuous operations

One-shot systems / Discrete operations

– Interoperability

Mission success usually requires a system to work with other systems. Characterizing the interfaces is important and the tester can help. For example, the AMRAAM missile ran into reliability problems late in the program and much of it had to be redesigned because the environment under the F-15 aircraft was not properly characterized. There was much more vibration than anticipated and the missile shook itself apart. This vibration level could have been measured and known in advance.

Built-in test

Indicators of maintenance action or upcoming mission failure are common in daily life. The gas gauge says it is time to fill up. The low-battery indicator on digital camera warns it is time to change batteries. In military systems built–in test capability extends this. Running the built in test confirms the system is ready or warns of a problem. BIT is usually a problem area.

BIT itself often fails. BIT says the system is not going to work but when the system is taken to maintenance, maintenance cannot duplicate the failure; or BIT says the system will work, but it fails.

How much of the system BIT actually checks is important to understand and assess. It is possible that the BIT does not look at the most important failure modes. Thus coverage of BIT should be tested.

There are choices in how to indicate upcoming required actions: BIT, idiot lights, gauges, voice, beeps… The effectiveness of these will have an important implication in mission success.

Use of new components versus use of known components

As part of the design process choices are made on the types of components that are used in the design. Some Components may have been used in similar systems and in similar environments. A lot is known about them; and there may be a great deal of confidence about what to expect in terms of performance and reliability. A new component for which no experience database exists will require more testing. Even a known component for which the environment is different would require more testing.

Non-developmental items (NDI) and

Commercial off the self (COTS) items

Most items that are called NDI or COTS require development and are not available commercially on any self. If a system is called NDI or COTS the first thing that needs to be determined is the amount of development and change in the product. If the product is NDI or COTS start testing right away. If it turns out the product is really not available, then find out what will change.

The USAF Firefly aircraft, which killed 4 or 6 student pilots and has been abandoned by the AF, is a good example of something that was labeled NDI but in fact had many new components, and was never operationally tested.

Component Reliability

The reliability budget specifies the reliability needed for each component. The reliability is dependent on the environment. This includes vibration, temperature, shock, power supply stability, electromagnetic, etc. All these effects must be understood. Often the subcontractor specification of the reliability of a subcomponent is provided under laboratory test conditions that are not at all like those that the component will experience in operational use. FMTV drive train was used outside of recommended specifications.

Interfaces

System architecture – upgradability

Systems integration Reliability

Physical integration

Example: AMRAAM under the F-15 could not take the vibration

Functional integration

MARs Lander had two components, one to determine the decent rate and a second to provide thrust to slow it down for a soft landing. One component provided the decent in meters and the thrust component expected the number to be supplied in feet.

Logistic support Reliability

Spare parts lists and stockage, special maintenance equipment, special tools, training, logistic downtime, total inventory and fraction of systems in "pipeline." Total number of parts, number of unique parts, unique federal stock number, number that will be contractor unique.

Life cycle Reliability

Architecture determines whether systems can be upgraded or will be replaced.

Lifecycle may be determined by obsolescence or by new threat.

Disposal is a problem. For example, batteries.

Reliability monitoring in the field and fleet

How often as configurations change?

Lot acceptance tests

Stockpile tests

Use of simulation

Reliability trends

Documentation

5. Framework for Evaluating Reliability

Types of Reliability Failures

Mission Failures

System failures

Unscheduled spares Demands

Infant Mortality

Wear out

Failure under stress

Environmental

cold weather

jungle - tropic

desert - sand

Other / Random

Operational Loads

Operational Environments

Component Evaluation

Components that are known

Components that are new

Defining Failure Modes

Integration Testing

MARs Lander had two components, one to determine the decent rate and a second to provide thrust to slow it down for a soft landing. One component provided the decent in meters and the thrust component expected the number to be supplied in feet.

GPS user equipment worked on the bench but did not work when in the F16.

System Level Testing

Repairable Systems / Continuous operations

One-shot systems / Discrete operations

6. Types of Reliability Testing

Development

Component testing

acceptance

Screening

Integration

System Level tests

Fixed configuration tests

Allowing the configuration to change

Growth tests

Continuous tests

7. Role of Modeling and Simulation in Reliability

Reliability Growth Modeling

The best use of RGM is to estimate the amount of test time (or number of test events) needed to reach a level of acceptable reliability for going to the field or to go to operational test.

RGPrograms used to begin at 30% of the desired reliability. It is now possible using modeling simulation, careful characterization of components and environments, expert opinion, etc, to begin at 70% of desired reliability in the first prototype. The early work, while it is resource intensive is not time intensive. So the advantage is that there is less test-fix-test to get to the desired reliability.

Reliability Growth Modeling of Repairable Systems

Reliability Growth Modeling of One-shot Systems

8. Software "Reliability"

Appendices

A1. Failure Review Boards and FRACAS Process